2021 XVII International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY) | 978-1-6654-3308-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/REDUNDANCY52534.2021.9606472

On Squares of Dihedral Codes

Kirill Vedenev
Department of Algebra and Discrete Mathematics
Southern Federal University
Rostov–on–Don, Russia
vedenevk@gmail.com

Yury Kosolapov
Department of Algebra and Discrete Mathematics
Southern Federal University
Rostov–on–Don, Russia
itaim@mail.ru

***Abstract*—The Schur–Hadamard squares are of particular interest due to its cryptographic applications. Namely, many attacks on code–based public–key encryption protocols have been constructed by employing Schur–Hadamard product. In addition, the specific properties of Schur–Hadamard squares of codes play an important role in building linear secret sharing and secure multi-party computation protocols. In this paper, we prove that the Schur–Hadamard products of group codes are group codes. Next, we consider the Schur–Hadamard product of the dihedral codes, i.e. the left ideal of dihedral group algebras. We obtain explicit algebraic description of the primitive dihedral codes products. Next, this result is applied to describe the squares of dihedral codes.**

***Index Terms*—Schur–Hadamard product, dihedral codes, group codes, group algebras, Fourier Transform**

INTRODUCTION

A. Motivation and background

Recall that a linear $[n,k]_q$ – code C of length n over the Galois field $\mathbb{F}_q$ is a linear subspace of dimension k of the space $\mathbb{F}_q^n$. Codes are used not only to protect data from errors in data transmission channels and data storage systems. In the field of secure communication and secure computation, they are applicable in various protection schemes. In combinatorial steganography, linear codes are used to minimize changes in the stego-containers [1] and to defend against an active adversary [2]. For copyright protection, linear codes are used to construct broadcast encryption schemes and to trace pirates (see [3]–[6]). In addition, linear codes are also used to construct linear secret sharing schemes (see [7]–[10]). Such schemes, in turn, are the basis for some secure multiparty computation schemes [11]. With code-based encryption protocols being one of the main approaches to build quantum computer–resistant public–key encryption (see e.g. [12]), the study of specific properties of codes related to this applications have gained particular interest recently. Note that one of the finalists of NIST post–quantum cryptography competition is the McEliece cryptosystem based on linear Goppa codes [13], with large public keys being its main drawback. It is believed that this drawback can be fixed by replacing Goppa codes with other classes of codes.

The use of linear error-correcting codes in the security schemes noted above makes it possible to describe the properties of new protection constructions and schemes using geometric and algebraic characteristics of the code C lying in their basis. These characteristics include minimum code distance, coverage radius, structure of generator and parity matrices, groups of permutation automorphisms, code decomposability etc. In a number of cases, information on the properties of a protection scheme is provided not only by the characteristics of C. Important information can be obtained by examining the characteristics of the code C^2 obtained by C using the Schur-Hadamard product. Recall that for two vectors $\mathbf{a} = (a_1, ..., a_n)$ and $\mathbf{b} = (b_1, ..., b_n)$ their Schur-Hadamard product is a vector $\mathbf{a} \star \mathbf{b} = (a_1 b_1, ..., a_n b_n)$ obtained by coordinatewise multiplication. Hence for two linear codes $C_1, C_2 \subset \mathbb{F}_q^n$ their Schur-Hadamard product code $C_1 \star C_2$ is defined as the $\mathbb{F}_q$–linear span of the set $\{\mathbf{c}_1 \star \mathbf{c}_2 \mid \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\}$ [14]. The Schur-Hadamard square (hereinafter simply the square) of the code C is the code $C^2 = C \star C$.

In [15] it was shown that with a high probability the dimension of the square of a randomly and uniformly chosen $[n,k]_q$-code is equal to $k(k+1)/2$. In [16], for the generalized Reed-Solomon (GRS) code it was shown that the square of GRS code is also GRS code of higher dimension. For binary Reed-Muller (RM) codes in [17] it was proved that the square of these codes are RM codes with double order. In [18] and [19], the explicit knowledge of dimensions of the squares of the GRS code and binary RM code, respectively, allowed constructing attacks on the modification of the McEliece-type cryptosystem, in which random columns are mixed with columns of generator matrix. In [16], it was also established that the square of the subcode of the GRS code is most likely a GRS code of higher dimension. A similar result was obtained in [20] for subcodes of a binary RM code of codimension one. The results of [16] and [20] made it possible to reduce the attacks on McEliece-type cryptosystems based on subcodes to the well-known Sidelnikov-Shestakov attack [21] (in GRS code case) and to the well-known Minder-Shokrollahi [22] and Chizhov-Borodin [17] attacks (in binary RM code case). In [23] the decomposability of the square code into a direct sum of the codes made it possible to construct an attack on Sidelnikov's cryptosystem based on repetition of binary RM codes [24], and to refine the security of the generalization of this system constructed in [25].

The importance of studying the properties of code squares for specific classes of codes is due not only to the search for suitable codes for code cryptosystems. For example, in [26] it was established that the multiplicativity index of secret sharing schemes depends on the dual distance of the code used, as well

as on the minimum code distance of the square of this code.

As noted above, the properties of squares have been most studied for GRS and RM codes and constructions based on them. Also some important properties of squares have been studied for cyclic codes. Namely, in [27] it was shown that the squares of cyclic codes are cyclic, and also a explicit description of their generating polynomials was obtained and their dimension was calculated. Note that the problem of describing the algebraic and geometric characteristics of C^2, even if such characteristics for C are known, is generally difficult. The algebraic structure of the code C can simplify the study of such characteristics. In this paper, the main focus is devoted to studying squares of group codes, namely, the squares of dihedral group codes.

B. Group algebras and group codes

Let G be a finite group. Recall that the $\mathbb{F}_q$-vector space

$$\mathbb{F}_q G := \left\{ \sum_{g\in G} \alpha_g g \mid \alpha_g \in \mathbb{F}_q \right\}$$

with the basis $\{g \in G\}$ and the multiplication operation

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g,$$

is called *group algebra for group G over field $\mathbb{F}_q$* ([28], p. 131). Any one-sided ideal I of the algebra $\mathbb{F}_q G$ is called a *group code* or simply a *G-code*. A G–code C is called *abelian* if G is abelian, otherwise C is called *non–abelian*. Many classical codes such as cyclic codes, Reed-Solomon codes and Reed-Muller codes are known to be abelian group codes (see [29], [30]). But since non-abelian group algebras have much richer algebraic structure, non–abelian group codes are of particular interest.

An important example of non–abelian group codes that have been already constructed is dihedral group codes, i.e. the left ideals of $\mathbb{F}_q D_n$, where $D_n = \langle a, b \mid a^n, b^2, a^i b = ba^{-i}\rangle$. Namely, in [31] the explicit algebraic description of this codes was obtained in the case when $\gcd(q, 2n) = 1$. In [32] for any dihedral code a generating idempotent was constructed and several classes of induced dihedral codes were studied. In [33] the explicit algebraic description of the D_n–codes and their duals was obtained in the case when $\gcd(q, n) = 1$. In addition, bases, generator and check matrices were constructed and several estimates of code parameters were obtained.

In this paper, we obtain the algebraic description of the squares of D_n–codes in the case when $\gcd(q, n) = 1$. *Hereinafter in this paper we assume that* $\gcd(q, n) = 1$.

C. The structure of paper

This paper is organized as follows. In Section I, we give some necessary preliminaries on dihedral codes (D_n–codes), cyclic group algebras, the Finite Fourier Transform, and cyclotomic cosets. In Section II, we prove that Schur–Hadamard product of any G–codes is also a G–code for any group G and provide its basic algebraic description. In Section III, we calculate the explicit algebraic description of Schur–Hadamard product of primitive dihedral codes. Finally, in Section IV, given a D_n–code we obtain the description of its square.

I. Preliminaries

In this section, we give some necessary preliminaries on cyclic group algebras, Fourier Transform, and dihedral codes.

A. Cyclic group algebras

Let $C_n = \langle h \mid h^n\rangle$ be a cyclic group of order n with generator h. Consider an algebra $\mathbb{F}_q C_n$. Any element $u \in \mathbb{F}_q C_n$ can be represented as

$$u = \sum_{i=0}^{n-1} P_i h^i = P(h),\ P(x) \in \mathbb{F}_q[x],\ \deg P(x) \le n-1. \tag{1}$$

Let $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$. As is well–known, the map

$$P(x) + (x^n - 1) \mapsto P(h) : \quad \mathcal{R}_n \to \mathbb{F}_q C_n$$

is a $\mathbb{F}_q$–algebras isomorphism . Recall that any ideal of $\mathbb{F}_q C_n$ is called a cyclic code.

Given a polynomial $g(x) = \sum_{i=0}^{\deg g} g_i x^i \in \mathbb{F}_q[x]$, by $g'(x)$ we denote its derivative, i.e.

$$g'(x) = \sum_{i=1}^{\deg(g)} g_i i x^{i-1}.$$

For a polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(0) \neq 0$, g^* denotes the reciprocal polynomial, e.g. $g^*(x) = x^{\deg g} g(x^{-1})$. A polynomial g is said to be auto-reciprocal if g and g^* have the same roots in their splitting field.

Recall that an element i in a ring R is called *an idempotent* if $i^2 = i$. In [34] it was proved that for any monic divisor $g(x)$ of the polynomial $x^n - 1$, the element

$$e_g(x) := -\frac{x^{\deg(g)-1}\left((g^*)'(x^{-1})\right)}{n} \cdot \frac{x^n - 1}{g(x)} \tag{2}$$

is an idempotent of the ring $\mathcal{R}_n$, with $e_g(x)$ generating the left ideal $\mathcal{R}_n e_g(x) = \mathcal{R}_n \frac{(x^n-1)}{g(x)}$. Note that since $\mathcal{R}_n$ and $\mathbb{F}_q C_n$ are isomorphic, it follows that $e_g(h)$ is also an idempotent of $\mathbb{F}_q C_n$. In addition, $e_g(h^{-1}) = e_{g^*}(h)$.

Lemma 2 of [32] yields that for any root α of $x^n - 1$ we have

$$e_g(\alpha) = \begin{cases} 1, & g(\alpha) = 0 \\ 0, & g(\alpha) \neq 0 \end{cases}. \tag{3}$$

B. Fourier Transform

Let $n \mid (q-1)$ and let $\omega \in \mathbb{F}_q$ be a primitive n–root of 1. The map

$$\mathcal{F}_\omega : \mathbb{F}_q C_n \to \mathbb{F}_q C_n, \quad P(h) \mapsto \sum_{i=0}^{n-1} P(\omega^i) h \tag{4}$$

is called the Discrete Fourier Transform with respect to ω [35]. As is well–known this transform has the following properties (see [35])

1) $\mathcal{F}_\omega^{-1} = (1/n)\mathcal{F}_{\omega^{-1}}$;
2) $\mathcal{F}_\omega(u+v) = \mathcal{F}_\omega(u) + \mathcal{F}_\omega(v)$ and $\mathcal{F}_\omega(\lambda u) = \lambda\mathcal{F}_\omega(u)$ for any $u, v \in \mathbb{F}_q C_n, \lambda \in \mathbb{F}_q$;
3) $\mathcal{F}_\omega(uv) = \mathcal{F}_\omega(u) \star \mathcal{F}_\omega(v)$ and $\mathcal{F}_\omega(u \star v) = \mathcal{F}_\omega(u)\mathcal{F}_\omega(v)$ for any $u, v \in \mathbb{F}_q C_n$, where $u \star v$ denotes group algebra Schur–Hadamard product, i.e.

$$\left(\sum_{g\in G} u_g g\right) \star \left(\sum_{g\in G} v_g g\right) = \left(\sum_{g\in G} (u_g v_g) g\right).$$

C. Factorization of $x^n - 1$ and cyclotomic cosets

Let $\gcd(q, n) = 1$. Let ω be a primitive n–root of 1 in the splitting field of $x^n - 1$ over $\mathbb{F}_q$. By $[u]$ we denote q–cyclotomic coset of u, i.e.

$$[u] = \{uq^i \in \mathbb{Z}_n \mid i \geq 0\}.$$

By $f_u(x) \in \mathbb{F}_q[x]$ we denote the minimal monic polynomial of $\alpha_u := \omega^u$. As is well–known, $f_u(x) = \prod_{t\in[u]}(x - \omega^t)$. Note that definition of auto–reciprocal polynomials and proprieties of cyclotomic cosets imply that f_u is auto–reciprocal if and only if $-u \in [u]$. Moreover, $f_u^*(x) = f_{-u}(x)$.

Recall that $x^n - 1$ can be factorised into monic irreducible factors over $\mathbb{F}_q$ as follows

$$x^n - 1 = \prod_{[u]\subset\mathbb{Z}_n} f_u(x). \tag{5}$$

D. Dihedral group codes

In [31]–[33] the algebraic description of dihedral codes has been obtained. Below we present this result in the convinient form.

Recall that the dihedral group D_n has the following presentation $D_n = \langle a, b \mid a^n, b^2, a^i b = ba^{-i}\rangle$. Hence any element $w \in \mathbb{F}_q D_n$ can be written as follows

$$w = P(a) + bQ(a) = P(a) + Q(a^{-1})b,$$

where $P(x), Q(x) \in \mathbb{F}_q[x]$ and $\deg P < n$, $\deg Q < n$ [33]. In addition, clearly

$$aw = aP(a) + ba^{-1}Q(a), \quad bw = Q(a) + bP(a).$$

Let $P, Q \in \mathbb{F}_q C_n$, let $u \in \mathbb{Z}_n$. Define

$$\mathcal{I}_u(P, Q) := (\mathbb{F}_q D_n)\left(P(a)e_{f_u}(a) + bQ(a)e_{f_u^*}(a)\right), \tag{6}$$

$$A_u := \mathcal{I}_u(0, 1) + \mathcal{I}_u(1, 0). \tag{7}$$

The codes $\mathcal{I}_u(P, Q)$ are called primitive dihedral codes.

Remark 1. *Since $f_u^* = f_{-u}$, it follows that $\mathcal{I}_u(P, Q) = b\mathcal{I}_u(P, Q) = \mathcal{I}_{-u}(Q, P)$.*

Remark 2. *Let $u \in \mathbb{Z}_n$, and $P, Q, R, S \in \mathbb{F}_q[x]$. If there exists $\lambda \in \mathbb{F}_q[\alpha_u]$ such that $\big(P(\alpha_u), Q(\alpha_u^{-1})\big) = \big(R(\alpha_u), S(\alpha_u^{-1})\big)$, then $\mathcal{I}_u(P, Q)$ and $\mathcal{I}_u(R, S)$ coincide. Hence it is useful to always assume that $\deg P < \deg f_u$, $\deg Q < \deg f_u$.*

Remark 3. *Let $\lambda, \mu \in \mathbb{F}_q$, $(\lambda, \mu) \neq (0, 0)$, $\lambda \neq \pm\mu$. If $f_u = x - 1$ or $f_u = x + 1$, then $\mathcal{I}_u(\lambda, \mu) = A_u$.*

Remark 4. *If f_u is auto–reciprocal, then $\mathcal{I}_u(P, Q) = A_u$ if and only if $P(\alpha_u)Q(\alpha_u) \neq P(\alpha_u^{-1})Q(\alpha_u^{-1})$.*

Theorem 1. *Let $\gcd(q, n) = 1$. Then any D_n–code C can be decomposed into inner direct sum of primitive codes as follows*

$$C = \sum_{j=1}^{k} \mathcal{I}_{u_j}(P_j, Q_j), \tag{8}$$

where $P_j, Q_j \in \mathbb{F}_q[x]$.

II. Schur–Hadamard product of group codes

In this section we prove that the Schur-Hadamard product of G–codes is a G–code and give algebraic description of it.

Lemma 1. *Let $\mathbb{F}_q G$ be a finite group algebra and let $A, B \in \mathbb{F}_q G$. Then for any $g \in G$ we have*

$$g(A \star B) = (gA) \star (gB).$$

Proof. Indeed,

$$g(A\star B) = g\sum_{h\in G} A_h B_h h = \sum_{h\in G} A_{g^{-1}h} B_{g^{-1}h} h = (gA)\star(gB).$$

□

Theorem 2. *Let $A, B \in \mathbb{F}_q G$ be zero–divisors in $\mathbb{F}_q G$ and let $C_1 = (\mathbb{F}_q G)A$, $C_2 = (\mathbb{F}_q G)B$ be G–codes generated by A, B. Then $C_1 \star C_2$ is a G–code and*

$$C_1 \star C_2 = \sum_{g\in G} (\mathbb{F}_q G)\left(A \star (gB)\right) = \sum_{g\in G} (\mathbb{F}_q G)\left((gA) \star B\right).$$

Proof. Clearly, the codes C_1 and C_2 are $\mathbb{F}_q$–linear spans of

$$T_1 = \{gA \mid g \in G\}, \quad T_2 = \{gB \mid g \in G\}.$$

It follows that $C_1 \star C_2$ is $\mathbb{F}_q$–linear span of

$$T_3 = \{(gA) \star (hB) \mid g, h \in G\}.$$

To prove that $C_1 \star C_2$ is a G–code, it is enough to verify that $kt \in C_1 \star C_2$ for any $k \in G$ and $t \in T_3$. Indeed, let $t = (gA) \star (hB)$. Using Lemma 1, we obtain

$$k\left((gA) \star (hB)\right) = (kgA) \star (khB) \in T_3 \subset C_1 \star C_2.$$

So, $C_1 \star C_2$ is a G–code.

Since $C_1 \star C_2 = (\mathbb{F}_q G)T_3$ and

$$T_3 = \{(gA) \star (hB) \mid g, h \in G\} = \{g\left(A \star (hB)\right) \mid g, h \in G\},$$

it follows that

$$C_1\star C_2 = \sum_{h\in H}\sum_{g\in G} (\mathbb{F}_q G)g\left(A \star (hB)\right) = \sum_{h\in G} (\mathbb{F}_q G)(A\star(hB)).$$

Due to symmetry we have $C_1 \star C_2 = \sum_{g\in G}(\mathbb{F}_q G)(gA \star B)$. This concludes the proof of the theorem. □

Remark 5. *The procedure for finding generating elements of $C_1 \star C_2$ can be simplified as follows. Let B_2 be a $\mathbb{F}_q$–basis of C_2. Then*

$$C_1 \star C_2 = \sum_{u\in B_2} (\mathbb{F}_q G)(A \star u).$$

Note that sometimes it is more convenient to describe Schur–Hadamard product of group codes over some extension of the field $\mathbb{F}_q$, i.e. using the Fourier Transform. In the following theorem, we give a framework to study the Schur–Hadamard products of group codes over $\mathbb{F}_q$ by studying the Schur–Hadamard products of codes over an extension $\mathbb{F}_q^t$.

Theorem 3. *Let $C_1, C_2 \subset \mathbb{F}_q G$, let $t \in \mathbb{N}$. Then*

$$C_1 \star C_2 = (\mathbb{F}_q G) \cap \left(\hat{C}_1 \star \hat{C}_2 \right),$$

with $\hat{C}_i = \mathbb{F}_{q^t} \otimes_{\mathbb{F}_q} C_i$, $i = 1, 2$, being G–codes over $\mathbb{F}_{q^t}$.

Proof. Clearly, C_i are codes in $\mathbb{F}_{q^t} G$. In addition, we have

$$(\mathbb{F}_{q^t} \otimes_{\mathbb{F}_q} C_i) \cap \mathbb{F}_q G = C_i.$$

The propreties of Schur–Hadamard imply that

$$\hat{C}_1 \star \hat{C}_2 = \mathbb{F}_{q^t} \otimes_{\mathbb{F}_q} (C_1 \star C_2).$$

Hence $C_1 \star C_2 = (\hat{C}_1 \star \hat{C}_2) \cap \mathbb{F}_q G$. □

III. Schur–Hadamard product of primitive dihedral codes

In this section, given two primitive D_n–codes $\mathcal{I}_u(P, Q)$ and $\mathcal{I}_v(R, S)$, we obtain explicit algebraic description of their Schur–Hadamard product by using the results of Section II. For the sake of simplicity and clarity, we consider the case when $n \mid q - 1$ first due to nice–looking results. Next, we consider the general case when $\gcd(q, n) = 1$.

A. Case $n \mid q - 1$

Note that in the case $n \mid q-1$ all polynomials in factorization of $x^n - 1$ are of degree 1. It follows that, without loss of generality, we may assume $P, Q, R, S \in \mathbb{F}_q$ (see Remark 2).

Lemma 2. *Consider $\mathbb{F}_q C_n$, $n \mid q - 1$. Then for any $\lambda(x), \mu(x) \in \mathbb{F}_q[x]$ we have*

$$(\lambda(a) e_{x-\omega^i}(h)) \star (\mu(a) e_{x-\omega^i}(h)) = \lambda(\omega^i)\mu(\omega^j) e_{x-\omega^{i+j}}(h).$$

Proof. Indeed, (4) and (3) imply that

$$\mathcal{F}_\omega \left(\lambda(h) e_{x-\omega^i}(h) \right) = \lambda(\omega^i) h^i,$$
$$\mathcal{F}_\omega \left(\mu(h) e_{x-\omega^j}(h) \right) = \mu(\omega^j) h^j.$$

Hence using properties of the Fourier Transform listed in Sec. I, we obtain

$$\begin{aligned} &\left(\lambda(\omega^i) e_{x-\omega^i}(h)\right) \star \left(\mu(\omega^j) e_{x-\omega^i}(h)\right) = \\ &= \mathcal{F}_\omega^{-1}(\lambda(\omega^i) h^i) \star \mathcal{F}_\omega^{-1}(\mu(\omega^j) h^j) = \\ &= \lambda(\omega^i)\mu(\omega^j) \mathcal{F}_\omega^{-1}(h^i h^j) = \lambda(\omega^i)\mu(\omega^j) e_{x-\omega^{i+j}}(h). \end{aligned}$$

□

Theorem 4. *Let $n \mid q - 1$, $u, v \in \mathbb{Z}_n$. Let $P, Q, R, S \in \mathbb{F}_q$. Then*

$$\mathcal{I}_u(P, Q) \star \mathcal{I}_v(R, S) = \mathcal{I}_{u+v}(PR, QS) + \mathcal{I}_{u-v}(PS, QR).$$

Proof. Recall that

$$\mathcal{I}_u(P, Q) = (\mathbb{F}_q D_n) \left(P e_{f_u}(a) + bQ e_{f_u^*}(a) \right),$$
$$\mathcal{I}_v(R, S) = (\mathbb{F}_q D_n) \left(R e_{f_v}(a) + bS e_{f_v^*}(a) \right).$$

Hence using Theorem 2, we obtain

$$\begin{aligned} &\mathcal{I}_u(P, Q) \star \mathcal{I}_v(R, S) = \\ &= \sum_{k=0}^{n-1} \sum_{z=0}^{1} (\mathbb{F}_q D_n) \Big((P e_{f_u}(a) + bQ e_{f_u^*}(a)) \star \\ &\qquad \star a^k b^z (R e_{f_v}(a) + bS e_{f_v^*}(a)) \Big) = \\ &= \sum_{k=0}^{n-1} (\mathbb{F}_q D_n) \Big((P e_{f_u}(a) \star a^k R e_{f_v}(a)) + \\ &\qquad + b(Q e_{f_u^*}(a) \star a^{-k} S e_{f_v^*}(a)) \Big) + \\ &+ \sum_{k=0}^{n-1} (\mathbb{F}_q D_n) \Big((P e_{f_u}(a) \star a^k S e_{f_v^*}(a)) + \\ &\qquad + b(Q e_{f_u^*}(a) \star a^{-k} R e_{f_v}(a)) \Big). \end{aligned}$$

Hence using Lemma 2 we obtain the claim of the theorem. □

B. General case

First consider the sum of cyclotomic cosets $[u], [v]$:

$$\begin{aligned} &[u] + [v] = \\ &= \{uq^i + vq^j \mid 0 \le i < \deg(f_u),\ 0 \le j < \deg(f_v)\} = \\ &= \{q^i(u + vq^j) \mid 0 \le i < \deg(f_u),\ 0 \le j < \deg(f_v)\} = \\ &= \bigcup_{j=0}^{\deg(f_v)-1} [u + vq^j]. \end{aligned}$$

So, $[u] + [v]$ is a union of cyclotomic cosets of the form $[u + vq^j]$ (note that some of them may coincide). By $\langle [u], [v] \rangle$ we denote partition of $[u] + [v]$ into distinct cyclotomic cosets, i.e.

$$[u] + [v] = \bigsqcup_{[t] \in \langle [u], [v] \rangle} [t].$$

Lemma 3. *Consider $\mathbb{F}_q C_n$. Let $u, v \in \mathbb{Z}_n$, $P(h), Q(h) \in \mathbb{F}_q C_n$. Then*

$$P(h) e_{f_u}(h) \star Q(h) e_{f_v}(h) = T(h),$$

$$T(h) = \sum_{[t] \in \langle [u], [v] \rangle} \left(\sum_{\substack{0 \le i < \deg(f_u) \\ 0 \le j < \deg(f_v) \\ uq^i + vq^j = t}} P(h^{q^i}) Q(h^{q^j}) \right) e_{f_t}(h).$$

Proof. Using (3), we obtain

$$e_{f_u}(\omega^i) = \begin{cases} 1, & i \in [u], \\ 0, & i \notin [u] \end{cases}.$$

It follows that applying the Fourier Transform (4), we get

$$\mathcal{F}_\omega(P(h)e_{f_u}(h)) = \sum_{i=0}^{n-1} P(\omega^i)e_{f_u}(\omega^i)h^i = \\ = \sum_{uq^i\in[u]} P(\alpha_u^i)h^{uq^i},$$

$$\mathcal{F}_\omega(Q(h)e_{f_v}(h)) = \sum_{i=0}^{n-1} Q(\omega^i)e_{f_v}(\omega^i)h^i = \\ = \sum_{vq^i\in[v]} Q(\alpha_v^i)h^{vq^i}.$$

So, using property 3) of the Fourier Transform, we obtain

$$\mathcal{F}_\omega\left(P(h)e_{f_u}(h)\star Q(h)e_{f_u}(h)\right) = \\ = \left(\sum_{uq^i\in[u]} P(\alpha_u^i)h^{uq^i}\right)\left(\sum_{vq^i\in[v]} Q(\alpha_v^i)h^{vq^i}\right) = \\ = \mathcal{F}_\omega(T(h)).$$

□

Theorem 5. *Let $u, v \in \mathbb{Z}_n$, $P(h), Q(h), R(h), S(h) \in \mathbb{F}_q C_n$. Then*

$$\mathcal{I}_u(P,Q)\star\mathcal{I}_v(R,S) = \\ = \sum_{k=0}^{|[v]|-1}\Big(\sum_{[t]\in\langle[u],[v]\rangle}\mathcal{I}_t(T_{1,k,t},T_{2,k,t}) + \\ + \sum_{[t]\in\langle[u],[-v]\rangle}\mathcal{I}_z(T_{3,k,t},T_{4,k,t})\Big),$$

where

$$T_{1,k,t} = \sum_{\substack{0\le i<\deg(f_u)\\ 0\le j<\deg(f_v)\\ uq^i+vq^j=t}} P(h^{q^i})R(h^{q^j})h^{kq^j},$$

$$T_{2,k,t} = \sum_{\substack{0\le i<\deg(f_u)\\ 0\le j<\deg(f_v)\\ uq^i+vq^j=t}} Q(h^{q^i})S(h^{q^j})h^{-kq^j},$$

$$T_{3,k,t} = \sum_{\substack{0\le i<\deg(f_u)\\ 0\le j<\deg(f_v)\\ uq^i-vq^j=t}} P(h^{q^i})S(h^{q^j})h^{kq^j},$$

$$T_{4,k,t} = \sum_{\substack{0\le i<\deg(f_u)\\ 0\le j<\deg(f_v)\\ uq^i-vq^j=t}} Q(h^{q^i})R(h^{q^j})h^{-kq^j}.$$

Proof. Using Theorem 2 and Remarks 2, 5, we obtain

$$\mathcal{I}_u(P,Q)\star\mathcal{I}_v(R,S) = \\ = \sum_{k=0}^{n-1}(\mathbb{F}_qD_n)\Big((P(a)e_{f_u}(a))\star(a^kR(a)e_{f_v}(a)) \\ + b((Q(a)e_{f_u^*}(a)\star(a^{-k}S(a)e_{f_v^*}(a))\Big) + \\ + \sum_{k=0}^{n-1}(\mathbb{F}_qD_n)\Big((P(a)e_{f_u}(a))\star(a^kS(a)e_{f_v^*}(a)) \\ + b((Q(a)e_{f_u^*}(a)\star(a^{-k}R(a)e_{f_v}(a))\Big).$$

Hence applying Lemma 3 we obtain the claim of the theorem. □

Remark 6. *Since any D_n–code is $\mathbb{F}_q$–linear subspace sum of primitive codes, it follows that the product of arbitrary D_n–codes can be easily computed using the results of this section.*

Example 1. *Let $q = 2$, $n = 9$. Then cyclotomic cosets are*

$$[0] = \{0\}, \quad [1] = \{1,2,4,8,7,5\}, \quad [3] = \{3,6\},$$

and $f_0 = x - 1$, $f_1 = x^6 + x^3 + 1$, $f_2 = x^2 + x + 1$ (see (5)). Consider $\mathcal{I}_1(P,Q)$ and $\mathcal{I}_3(R,S)$. Since $\langle[1],[3]\rangle = \langle[1],[-3]\rangle = [1]$ and

$$1 = 1\cdot 2^4 + 3\cdot 2^0 = 1\cdot 2^2 + 3\cdot 2^1 = \\ 1\cdot 2^4 - 3\cdot 2^1 = 1\cdot 2^2 - 3\cdot 2^0,$$

it follows that

$$\mathcal{I}_1(P,Q)\star\mathcal{I}_3(R,S) = \mathcal{I}_1(T_{1,0,1},T_{2,0,1}) + \\ + \mathcal{I}_1(T_{3,0,1},T_{4,0,1}) + \mathcal{I}_1(T_{1,1,1},T_{2,1,1}) + \mathcal{I}_1(T_{3,1,1},T_{4,1,1}),$$

where

$$T_{1,k,1} = P(h^{16})R(h)h^k + P(h^4)R(h^2)h^{2k},$$
$$T_{2,k,1} = Q(h^{16})S(h)h^{-k} + Q(h^4)S(h^2)h^{-2k},$$
$$T_{3,k,1} = P(h^{16})S(h^2)h^{2k} + P(h^4)S(h)h^k,$$
$$T_{4,k,1} = Q(h^{16})R(h^2)h^{-2k} + Q(h^4)R(h)h^{-k}.$$

IV. Squares of dihedral codes

As noted in introduction, the Schur–Hadamard squares of codes are of particular interest. In the following theorem, we give algebraic description of the square of arbitrary D_n–code.

Theorem 6. *Let C be a dihedral code with decomposition* (8)*. Then C^2 is a dihedral code such that*

$$C^2 = \sum_{i=1}^{k}\sum_{j=i}^{k}\mathcal{I}_{u_i}(P_i,Q_i)\star\mathcal{I}_{u_j}(P_j,Q_j),$$

with $\mathcal{I}_{u_i}(P_i,Q_i)\star\mathcal{I}_{u_j}(P_j,Q_j)$ being defined in Theorem 4 or Theorem 5 depending on q and n.

Proof. Indeed, decomposing the code into the sum of primitive codes and applying Theorem 4 in the case $n \mid q-1$ or Theorem 5 in the general case we obtain the claim of the theorem. □

Example 2. *Let $q = 11$, $n = 10$. Let $\omega \in \mathbb{F}_{11}$ be a primitive 10–root of 1, let $P_i, Q_i \in \mathbb{F}_q$, $i = 0, 1, 2$. Recall that $x^{10} - 1 = \prod_{i=0}^{9} f_i(x)$ with $f_i = (x - \omega^i)$. Consider the code*

$$C = \mathcal{I}_0(P_0, Q_0) + \mathcal{I}_1(P_1, Q_1) + \mathcal{I}_2(P_2, Q_2).$$

Then using Theorem 6 and Theorem 4, we obtain

$$\begin{aligned} C^2 = {} & \mathcal{I}_0(P_0^2, Q_0^2) + \mathcal{I}_1(P_0P_1, Q_0Q_1) + \mathcal{I}_2(P_0P_2, Q_0Q_2) + \\ & + \mathcal{I}_0(P_0Q_0, P_0Q_0) + \mathcal{I}_{-1}(P_0Q_1, Q_0P_1) + \mathcal{I}_{-2}(P_0Q_2, Q_0P_2) + \\ & + \mathcal{I}_2(P_1^2, Q_1^2) + \mathcal{I}_0(P_1Q_1, P_1Q_1) + \\ & + \mathcal{I}_3(P_1P_2, Q_1Q_2) + \mathcal{I}_{-1}(P_1Q_2, Q_1P_2) + \\ & + \mathcal{I}_4(P_2^2, Q_2^2) + \mathcal{I}_0(P_2Q_2, P_2Q_2), \end{aligned}$$

with $\mathcal{I}_{-u}(x, y) = \mathcal{I}_u(y, x)$ (see Remark 1).

REFERENCES

[1] W. Zhang, X. Zhang and S. Wang, "Maximizing steganographic embedding efficiency by combining Hamming codes and wet paper codes," In International Workshop on Information Hiding (pp. 60-71). Springer, Berlin, Heidelberg, May 2008.

[2] F. Galand, and G. A. Kabatiansky, "Coverings, centered codes, and combinatorial steganography," Problems of Information Transmission, vol. 45, no. 3, pp. 289–294, 2009.

[3] G. Kabatiansky, "Codes for copyright protection: the case of two pirates," Problems of Information Transmission, vol. 41, no. 2, pp.182–186, 2005.

[4] V. M. Deundyak, S.A. Yevpak and V.V. Mkrtichyan, "Analysis of properties of q-ary Reed–Muller error-correcting codes viewed as codes for copyright protection," Problems of Information Transmission, vol. 51, no. 4, pp. 398–408, 2015.

[5] E. E. Egorova, "Generalization of IPP codes and IPP set systems," Problems of Information Transmission, vol. 55, no. 3, pp. 241–253, 2019.

[6] G. A. Kabatiansky, "Traceability codes and their generalizations," Problems of Information Transmission, vol. 55, no. 3, pp. 283–294, 2019.

[7] R. McEliece, "On secret sharing and Reed-Solomon codes," Communications of the ACM, vol. 24, pp. 583–584, 1981.

[8] G. R. Blakley and G. A. Kabatianski, "Linear algebra approach to secret sharing schemes," Error Control, Cryptology, and Speech Compression, Lect. Notes Comput. Sci., vol. 829, pp. 33–40, 1994.

[9] M. van Dijk, "A linear construction of secret sharing schemes," Designs, Codes and Cryptography, vol. 12, pp. 161–201, 1997.

[10] R. Cramer, I. B. Damgård, N. Döttling, S. Fehr, and G. Spini, "Linear secret sharing schemes from error correcting codes and universal hash functions," In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, pp. 313–336, April 2015.

[11] R. Cramer and I. Damgård, "Multiparty computation, an introduction," In Contemporary cryptology, Birkhäuser Basel, pp. 41-87, 2005.

[12] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. http://csrc.nist.gov/projects/post-quantum-cryptography. Updated: June 14, 2021.

[13] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, pp. 114–116, 1978.

[14] H. Randriambololona, "On products and powers of linear codes under componentwise multiplication," Algorithmic arithmetic, geometry, and coding theory, vol. 637, pp. 3–78, 2015.

[15] I. Cascudo, R. Cramer, D. Mirandola and G. Zémor, "Squares of random linear codes," IEEE Transactions on Information Theory, vol. 61, no. 3, pp. 1159-1173, 2015.

[16] C. Wieschebrink, "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes," In International Workshop on Post-Quantum Cryptography, Springer, Berlin, Heidelberg, pp. 61-72, May 2010.

[17] I. V. Chizhov and M. A. Borodin, "Effective attack on the McEliece cryptosystem based on Reed-Muller codes," Discrete Math. Appl, vol. 24, no. 5, pp. 273-280, 2014.

[18] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani and J. P. Tillich, "Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes," Designs, Codes and Cryptography, vol. 73, no. 2, pp. 641–666, 2014.

[19] A. Otmani and H. T. Kalachi, "Square code attack on a modified Sidelnikov cryptosystem," In International Conference on Codes, Cryptology, and Information Security, Springer, Cham, pp. 173–183, May 2015 May.

[20] I. V. Chizhov and M. A. Borodin, "Hadamard products classification of subcodes of Reed–Muller codes codimension 1," Diskretnaya Matematika, vol. 32, no. 1, pp. 115–134, 2020.

[21] V. M. Sidel'nikov and S. O. Shestakov, "On an encoding system constructed on the basis of generalized Reed–Solomon codes," Diskretnaya Matematika, vol. 4, no. 3, pp. 57–63, 1992.

[22] L. Minder and A. Shokrollahi, "Cryptanalysis of the Sidelnikov cryptosystem," In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, pp. 347–360, May 2007.

[23] V. M. Deundyak, Y. V. Kosolapov and I. A. Maystrenko, "On the Decipherment of Sidel'nikov-Type Cryptosystems," In Code-Based Cryptography Workshop, Springer, Cham, pp. 20–40, May 2020.

[24] V. M. Sidelnikov, "Public-key cryptosystem based on binary Reed-Muller codes," Discr. Math. and Applications, vol. 4, no. 3, pp. 191–208, 1994.

[25] G. Kabatiansky, C. Tavernier, "A new code-based cryptosystem via pseudorepetition of codes," Proceedings of ACCT XVI, pp. 189-191, September 2018.

[26] I. Cascudo, R. Cramer, D. Mirandola, C. Padró and C. Xing, "On secret sharing with nonlinear product reconstruction," SIAM Journal on Discrete Mathematics, vol. 29, no. 2, pp. 1114–1131, 2015.

[27] I. Cascudo, I, "On squares of cyclic codes," IEEE Transactions on Information Theory, vol. 65, no. 2, pp. 1034–1047, 2018.

[28] C. P. Milies, S. K. Sehgal, "An introduction to group rings. Vol. 1," Springer Netherlands, 371 p., 2002.

[29] A. V. Kelarev and P. Solé, "Error-correcting codes as ideals in group rings," *Contemporary Mathematics*, vol. 273, pp. 11–18, 2001.

[30] E. Couselo, S. González, V. T. Markov, C. Martínez, and A. A. Nechaev, "Ideal representation of Reed–Solomon and Reed–Muller codes," *Algebra and Logic*, vol. 51, no. 3, pp. 195–212, 2012.

[31] K. V. Vedenev and V. M. Deundyak, "Codes in a dihedral group algebra," *Automatic Control and Computer Sciences*, vol. 53, no. 7, pp. 745–754, Dec 2019.

[32] ——, "Relationship between codes and idempotents in a dihedral group algebra," *Mathematical Notes*, vol. 107, no. 1, pp. 201–216, 2020.

[33] ——, "Some properties of dihedral group codes," *arXiv preprint arXiv:2005.08283*, 2020.

[34] F. E. Brochero Martínez, "Structure of finite dihedral group algebra," *Finite Fields and Their Applications*, vol. 35, pp. 204 – 214, 2015.

[35] J. L. Massey and S. Serconek, "Linear complexity of periodic sequences: a general theory," in *Annual International Cryptology Conference*. Springer, 1996, pp. 358–371.